UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

DEIDRA CLAY, individually and on behalf of all others similarly situated, Plaintiff, v. CARESOURCE, Defendant.	Case No. 1:23-cv-1868 CLASS ACTION COMPLAINT JURY DEMAND

Plaintiff **Deidra Clay** ("Plaintiff") brings this class action against Defendant **CareSource** ("Defendant" **of "CareSource"**) for its failure to properly secure and safeguard Plaintiff's and Class Members' protected health information ("PHI") stored within Defendant's information network.

INTRODUCTION

1. This lawsuit seeks to redress the harms caused by CareSource's massive and preventable data breach perpetrated by well-known cybergang, Cl0p ("Clop"). During the data breach Clop infiltrated the inadequately protected MOVEit software CareSource negligently used and stole the highly sensitive and confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") of Plaintiff and more than three million other similarly situated individuals (the "Class" or "Class Members").[1] Due to CareSource's failure to utilize software with adequate data security measures in place, Plaintiff and the Class face a lifetime risk of fraud and identity theft.

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (CareSource)

2. Defendant is a managed care organization based in Dayton, Ohio.[2] CareSource administers one of the largest Medicaid managed care plans in the country and offers health insurance to patients.[3] CareSource employs more than 4,700 people and generates more than $13 billion in annual revenue.[4]

3. On September 14, 2023, Defendant sent a letter to Plaintiff announcing a security breach of the data the Plaintiff and the Class had entrusted Defendant with (the "Data Breach" or "Breach").[5]

4. CareSource divulged that on or around May 31, 2023, a vulnerability in the MOVEit web transfer application that CareSource utilizes for transferring documents was hacked.

5. According to CareSource, it investigated its MOVEit database to assess its security and to identify whether any data had been stolen. By June 27, 2023, CareSource confirmed that Plaintiff and the Class's data had been stolen.[6]

6. CareSource admits that the information compromised in the Data Breach included PII and PHI such as Class Members' full name, address, date of birth, gender, Social Security number, member identification number, plan name, health conditions, medications, allergies, and diagnoses.[7]

---

[2] https://www.caresource.com/newsroom/fact-sheets/company-fact-sheet
[3] *Id.*
[4] *Id.*
[5] An unindividualized version of the letter sent to Plaintiff is available online at https://www.caresource.com/about-us/legal/corporate-compliance/vendor- compliance/hipaa-hitech/cybersecurity-incident/
[6] *Id.*
[7] *Id.*

7. Despite learning of the Data Breach *more than two months* earlier, Defendant did not send a notice of data event letter ("Notice of Data Breach") to Plaintiff until on or around September 14, 2023.[8] Thus, cybercriminals were given a head start in misusing Plaintiff's and the Class's PII/PHI before they were even informed of what happened.

8. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

9. This Complaint is brought against Defendant because of its failure to safeguard the Private Information entrusted to it, and to remedy the harms suffered by Plaintiff and all others similarly situated.

10. Plaintiff and Class Members have suffered injuries as a result of the Defendant's negligent conduct, including: (i) the potential for Plaintiff's and Class Members' exposed Private Information to be sold and distributed on the dark web (if it has not been already), (ii) a lifetime risk of identity theft, sharing, and detrimental use of their sensitive information, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information, (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (v) the continued and increased risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect its customers' Private Information.

11. Plaintiff and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they are entitled to equitable and injunctive relief.

JURISDICTION AND VENUE

12. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

13. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

14. Defendant is routinely conducts business in the State where this district is located and has offices in Cleveland, Ohio. Therefore there are sufficient minimum contacts in this State, and Defendant has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

15. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Defendant does business in this Judicial District, including, but not limited to, through its offices in Mayfield Heights, Ohio.

THE PARTIES

Plaintiff Deidra Clay

16. Plaintiff Deirdra Clay is an adult individual and, at all relevant times herein, a resident and citizen of Ohio, residing in Greenfield, Ohio. Plaintiff is a victim of the Data Breach.

17. Plaintiff was a patient of Defendant's, and their information was stored with Defendant as a result of their dealings with Defendant.

18. As required in order to obtain services from Defendant, Plaintiff provided Defendant with highly sensitive personal, health, and insurance information, who then possessed and controlled it.

19. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

20. At all times herein relevant, Plaintiff is and was a member of each of the Classes.

21. Plaintiff received a letter from Defendant, dated September 14, 2023, stating that her PHI was involved in the Data Breach (the "Notice").

22. Plaintiff was unaware of the Data Breach—or even that Defendant had retained possession of her data until receiving that letter.

23. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self- monitoring her accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach. Indeed, Plaintiff has already spent many hours monitoring her credit as a result of this breach and has taken steps to freeze her credit in light of it.

24. Plaintiff was also injured by the material risk to future harm she suffers based on Defendant's breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given the size of the community Defendant serves, that some of the Class's information that has been exposed has already been misused.

25. Plaintiff has serious cause for concern and has already been injured, as since the breach has occurred she's received an uptick in spam calls and texts sent to her phone and has already received notifications that her information has been disseminated on the dark web, where malicious actors may seek to misuse her data.

26. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PHI—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

27. Plaintiff, as a result of the Data Breach, has increased anxiety for her loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling her PHI.

28. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PHI and financial information, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

29. Plaintiff has a continuing interest in ensuring that her PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant CareSource

30. Defendant CareSource is a managed care corporation incorporated in Ohio, with offices at 5900 Landerbrook Drive, Mayfield Heights, Ohio 44124.

31. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

32. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

33. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of herself and the following classes/subclass(es) (collectively, the "Class"):

Nationwide Class:

> All individuals within the United States of America whose PHI was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant beginning on or around May 31, 2023.

Ohio Subclass:

> All individuals within the State of Ohio whose PII/PHI was stored by Defendant and/or was exposed to unauthorized third parties as a result of the data breach experienced by Defendant beginning non or around May 13, 2023.

34. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be

excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

35. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

36. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

37. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Plaintiff Classes (which Plaintiff is informed and believes, and on that basis, alleges that the total number of persons is in the thousands of individuals and can be determined analysis of Defendant's records) are so numerous that joinder of all members is impractical, if not impossible.

38. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not limited to:

a. Whether Defendant had a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and/or safeguarding their PHI;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI had been compromised;

g. How and when Defendant actually learned of the Data Breach;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PHI of Plaintiff and Class Members;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

39. Typicality: Plaintiff's claims are typical of the claims of the Plaintiff Classes. Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

40. Adequacy of Representation: Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature.

41. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. Plaintiff anticipates no management difficulties in this litigation.

42. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

43. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

44. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

45. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

46. Unless a Class-wide injunction is issued, Defendant may continue failing to properly secure the PHI of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

47. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Federal Civil Procedure Rule 23(b)(2).

COMMON FACTUAL ALLEGATIONS

A. Background

48. Defendant CareSource is a company headquartered in Dayton, Ohio that touts itself as one of the nation's largest Medicaid managed care plans. CareSource offers a number of insurance plans in addition to Medicaid through the Health Insurance Marketplace, and also offers Medicare Advantage plans.[8]

49. CareSource is a sizeable and experienced company, with more than 30 years of experience and more than 4,700 employees serving millions of customers.[9]

50. To provide its services to individuals, CareSource stores, maintains, and uses the Private Information of Plaintiff and the Class Members, including their full name, address, date of birth, gender, Social Security number, member identification number, plan name, health conditions, medications, allergies, and diagnoses.

51. CareSource acknowledges how critical it is to safeguard this information— and, therefore, how devastating it is to individuals whose information has been stolen. CareSource makes the following covenants with its customers:[10]

a. "CareSource employees are trained on how to protect member information."

[8] https://www.caresource.com/about-us/

[9] https://www.caresource.com/newsroom/fact-sheets/company-fact-sheet/

[10] *See, e.g.*, https://www.caresource.com/about-us/legal/hipaa-privacy-practices/hipaa- privacy-practices-georgia-marketplace/

b. "CareSource makes sure that computers used by employees are safe by using firewalls and passwords."

c. "CareSource limits who can access member health information. We make sure that only those employees with a business reason to access information use and share that information."

d. "We are required by law to keep the privacy and security of your protected health information."

e. "We will let you know quickly if a breach occurs that may have compromised the privacy or security of your information."

52. On or around May 31, 2023, the MOVEit software that Defendant uses to share Class Members' data in order to manage their benefits was hacked by a malicious actor.[11] The MOVEit software is produced by Progress Software Corporation ("PSC").

53. CareSource states that it patched its software on June 1, 2023—the day after the breach.[12] This was too little and too late.

54. PSC reports that it alerted users of its software to take down traffic to MOVEit software "[p]romptly following discovery and escalation of the vulnerability," which was days earlier. PSC also reports that it published and released the patch on May 31, 2023.[13]

55. CareSource began an investigation on June 1, 2023, to determine whether information was stolen. By June 27, 2023, it was confirmed that data in CareSource's custody had been breached.[14]

[11] https://www.caresource.com/about-us/legal/corporate-compliance/vendor-compliance/ hipaa-hitech/cybersecurity-incident/
[12] https://www.caresource.com/about-us/legal/corporate-compliance/vendor-compliance/ hipaa-hitech/cybersecurity-incident/
[13] https://community.progress.com/s/article/MOVEit-Cloud-Info-Regarding-Critical-Vulnerability-May-2023
[14] *Id.*

56. Despite its agreement that "We will let you know quickly if a breach occurs that may have compromised the privacy or security of your information," CareSource did not send victims of the Data Breach a Notice of Data Breach Letter until more than two months later, on or about September 5, 2023.

57. Defendant's Notice of Data Breach admits that Plaintiff's and Class Members' Private Information was accessed by cybercriminals without authorization.

58. Cl0p accessed and acquired files in Defendant's computer systems containing the unencrypted PII/PHI of Plaintiff and Class Members.

59. Defendant utilized the file transfer service, MOVEit, as a web transfer application to transfer documents. Defendant utilized the software with disregard for its data security and infrastructure.

60. Defendant agreed to and undertook legal duties to maintain the Private Information of Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws. Defendant had obligations created by the FTC Act, HIPAA, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure. To this end, Defendant acknowledged that "[w]e are required by law to keep the privacy and security of your protected health information."

61. Defendant knew of its duties to Plaintiff and the Class Members, and the risks associated with failing to protect the Private Information entrusted to it. Defendant knew that if it did not select a vendor/software with adequate security that Plaintiff's and the Class's Private Information would be unlawfully exposed.

62. Defendant also knew that if it did not properly monitor and secure the systems

under its own control, including the MOVEit software and related systems and servers, the PII and PHI with which it was entrusted could be breached.

63. Upon information and belief, Defendant failed to reasonably secure its systems handling consumers' PII and PHI, including the MOVEit software it hosted. Defendant also unreasonably failed to monitor and oversee MOVEit's data security throughout its use of the software. Had Defendant acted reasonably with respect to this critically sensitive PII and PHI, Plaintiff's and the Class's Private Information would have never been exposed in the Data Breach.

64. The unencrypted Private Information of Plaintiff and Class Members will likely be or already is for sale on the dark web and may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can already access the Private Information of Plaintiff and Class Members.[15]

65. Defendant was negligent and did not use or implement reasonable security procedures, oversight, and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

66. Defendant was also negligent in that it did not use software with adequate data security. Defendant should have inquired about MOVEit's data security prior to entrusting Plaintiff's and the Class's PII and PHI to the software.

[15] Clop cyber gang claims MOVEit attack and starts harassing victims (June 7, 2023), available at https://www.computerweekly.com/news/366539357/Clop-cyber-gang-claims- MOVEit-attack-and-starts-harassing-victims; Clop names a dozen MOVEit victims, but holds back details (June 15, 2023), available at https://www.cybersecuritydive.com/news/clop-moveit-data-leaks-victims-named/ 653131/

67. Because Defendant had a duty to protect Plaintiff's and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

68. In October 2019, the Federal Bureau of Investigation published an article online titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[16]

69. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[17]

70. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[18]

---

[16] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), available at https://www.ic3.gov/Media/Y2019/PSA191002 (last viewed Sept. 20, 2023).

[17] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware- mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Sept. 20, 2023).

[18] U.S. CISA, Ransomware Guide – available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Sept. 20, 2023).

71. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting big companies such as Defendant and Defendant's clients, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant and Defendant's clients, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

72. Considering the information readily available and accessible on the internet before the Data Breach and Defendant's involvement in data breach litigation, Defendant, having elected to store the unencrypted Private Information of Plaintiff and Class Members with a third-party without first ensuring that the third party's system was secure, had reason to know that Plaintiff and the Class Members' Private Information was at risk for being shared with unknown and unauthorized persons.

73. Prior to the Data Breach, Defendant knew or should have known that it was responsible for confirming that MOVEit's systems were secure and capable of protecting Plaintiff's and the Class Members' Private Information.

74. Since the breach, Defendant continues to store confidential information, including Plaintiff's and Class Members' Private Information, and has failed to give adequate assurances that it has enhanced its security practices sufficiently to avoid another breach in the future.

B. Plaintiff's Experience

75. CareSource acquired Plaintiff's Private Information while providing managed care services for Plaintiff Clay's healthcare, pertaining both to Plaintiff's doctor visits and to her prescriptions.

76. Defendant acquired, collected, and stored Plaintiff's Private Information and negligently used the MOVEit software to transfer files containing Plaintiff's PII/PHI. Defendant was in possession of Plaintiff's Private Information before, during, and after the Data Breach.

77. Defendant was obligated by law, regulations, and guidelines to protect Plaintiff's and the Class's Private Information, and Defendant was required to ensure the MOVEit software was adequately protected with data security and infrastructure to protect Plaintiff's and the Class's Private Information.

78. Plaintiff received the Notice of Data Breach on or around September 14, 2023. The Notice stated that the information exposed in the breach included Plaintiff's full name, address, date of birth, gender, Social Security number, member identification number, plan name, health conditions, medications, allergies, and diagnoses. Now, for the rest of their lives, Plaintiff is at a significant risk of identity theft and fraud.

79. As a result of the Data Breach, Plaintiff was forced to spend time dealing with the consequences of the Data Breach, including time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts, and changing the passwords on several of her accounts. This time has been lost forever and cannot be recaptured.

80. Plaintiff is very careful about sharing her sensitive Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

81. As a direct and traceable result of the Data Breach, Plaintiff suffered actual damages such as: (i) lost time related to monitoring her accounts for fraudulent activity; (ii) loss of privacy due to her Private Information being exposed to cybercriminals; (iii) loss of the benefit of the bargain because Defendant did not adequately protect her Private Information; (iv)

emotional distress because identity thieves now possess her Private Information; (v) exposure to increased and imminent risk of fraud and identity theft now that her Private Information has been exposed; (vi) the loss in value of her Private Information due to her Private Information being in the hands of cybercriminals who can use it at their leisure; and (vii) other economic and non-economic harm.

82. Plaintiff has also experienced actual misuse of her Private Information. After the breach, Plaintiff experienced a significant increase in spam text messages, emails, physical mail, and calls to her landline and cell phone. Because Plaintiff is required by her work to be responsive to phone calls and cannot simply ignore them, these spam calls impose a significant interruption to Plaintiff's daily life.

83. The misuse of Plaintiff's Private information has caused her significant frustration and anxiety.

84. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and criminals.

85. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

C. Cyber Criminals Will Use Plaintiff's PII and PHI to Defraud Her

86. PII and PHI are of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and the Class Members to profit off their misfortune.

87. Each year, identity theft causes tens of billions of dollars of losses to victims in

the United States.[19] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[20] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

88. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:[21]

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.

(Emphasis added.)

89. PII and PHI are such valuable commodities to identity thieves that once this information has been compromised, criminals will use it for years.[22]

90. This was a financially motivated Breach, as the reason the cyber criminals go through the trouble of running a targeted cyberattack is to get information that they can monetize

---

[19] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").
[20] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 15, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity- thief-can-use-your-social-security-number/860643001/
[21] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you- should-know/.
[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

by selling it on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[23] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[24]

91. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[25]

92. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[26]

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

93. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[27]

94. The ramifications of Defendant's failure to keep its Class Members' PII secure

---

[23] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.
[24] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you- should-know/.
[25] Ari Lazarus (consumer education specialist, FTC), *How fast will identity thieves use stolen info?*, Military Consumer (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.
[26] Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO, June 4, 2007, https://www.gao.gov/assets/gao-07-737.pdf
[27] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 15, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity- thief-can-use-your-social-security-number/860643001/

are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for up to six to twelve months, or even longer.

95. The ramifications of Defendant's failure to keep its Class Members' PII secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for up to six to twelve months, or even longer.

96. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [30] This gives thieves ample time to commit multiple fraudulent activities, including seeking medical treatment under the victim's name. Forty percent (40%) of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[28]

97. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

98. Defendant's offer of two years of identity monitoring and protection services to Plaintiff and the Class is woefully inadequate and will not fully protect them from the damages and harm caused by Defendant's cybersecurity failures. While some harm has begun already, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. Once the twenty-four months have expired, Plaintiff and Class Members will need to pay

[28] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-

for their own identity theft protection and credit monitoring for the rest of their lives due to Defendant's negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[29] Nor can an identity monitoring service remove personal information from the dark web.[30] "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[31]

99. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach in their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more serious is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and Class Members must take.

---

[29] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be- worth-the-cost.html

[30] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you- should-know/.

[31] *Id.*

100. Plaintiff and Class Members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including PII/PHI;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

d. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves may use that information to defraud other victims of the Data Breach;

e. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach; and

f. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' personal information for which there is a well-established and quantifiable national and international market.

101. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown themselves wholly incapable of protecting Plaintiff's and Class Members' Private Information.

102. CareSource acknowledged the harm caused by the Data Breach because it

offered Plaintiff and Class Members the woefully inadequate twenty-four months of identity monitoring and protection services. Twenty-four months of identity monitoring and protection services is, however, insufficient to protect Plaintiff and Class Members from a lifetime of identity theft risk.

103. Defendant further acknowledged, in its letter to Plaintiff and other Class Members, that CareSource needed to improve its security protocols, stating: "We are doing a full investigation and are looking into what, if any, updated processes may be needed."[32]

104. The Breach Notice further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, telling Class Members to "Stay alert. Check your accounts for fraudulent activity."[33]

105. At Defendant's suggestion, Plaintiff and Class Members are desperately trying to mitigate the damage that Defendant's Data Breach has caused them. Given the kind of Private Information Defendant made accessible to hackers by utilizing the inadequately protected MOVEit software, Plaintiff and Class Members are certain to incur additional damages. Because identity thieves have their PII and PHI, Plaintiff and Class Members will need to have identity monitoring and protection services for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[34]

106. None of this should have happened.

---

[32] https://www.caresource.com/about-us/legal/corporate-compliance/vendor-compliance/ hipaa-hitech/cybersecurity-incident/

[33] *Id.*

[34] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security- number-affect-your-credit.html.

D. Defendant Was Aware of the Risk of Cyber Attacks

107. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[35] Yahoo,[36] Marriott International,[37] Chipotle, Chili's, Arby's,[38] and others.[39]

108. Defendant, who provides managed care services to companies throughout the United States requiring the collection and maintenance of highly sensitive and valuable PII and PHI, should certainly have been aware, and indeed was aware, that failing to ensure the MOVEit software employed minimum basic security precautions created a substantial risk for a data breach that could expose the Private Information it collected and maintained.

109. With the increasing prevalence of data breach announcements, Defendant certainly recognized it had a duty to use reasonable measures to protect the wealth of PII and PHI it collected and maintained.

110. In 2022, a total of 1,802 data breaches occurred, which represents the second highest number of data events in a single year and just 60 events short of the all-time record of

---

[35] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the- target-data-breach-missed-opportunities-and-lessons-learned/.

[36] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the- russian-hack-of-yahoo-how-they-did-it.html.

[37] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach- this-is-why-insurance-matters/.

[38] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in- theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[39] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data- breaches-of-the-21st-century.html.

1,862 in 2021.[40]

111. In light of the significant number of data breaches that occurred in 2022, Defendant knew or should have known that its customers' Private Information would be targeted by cybercriminals.

112. Defendant was clearly aware of the risks it was taking when it failed to ensure the MOVEit software provided sufficient cybersecurity protection, and of the harm that could result from inadequate data security.

E. Defendant Could Have Prevented the Breach

113. Data breaches are preventable.[41] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[42] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[43]

114. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[44]

115. In a Data Breach like this, many failures laid the groundwork for the Breach.

---

[40] ITRC_2022-Data-Breach-Report_Final-1.pdf (idtheftcenter.org)
[41] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[42] *Id.* at 17.
[43] *Id.* at 28.
[44] *Id.*

The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[45] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

116. Upon information and belief, Defendant failed to ensure that the MOVEit software maintained reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Defendant also failed to ensure that the MOVEit software met the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity preparation.

117. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[46]

---

[45] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[46] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/ view.

118. To prevent and detect cyber-attacks, including the attack that resulted in the Data Breach, Defendant could and should have implemented, or ensured that PSC implemented, as recommended by the Federal Bureau of Investigation, the following measures:[47]

> Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
>
> Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
>
> Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
>
> Configure firewalls to block access to known malicious IP addresses.
>
> Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
>
> Set anti-virus and anti-malware programs to conduct regular scans automatically.
>
> Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
>
> Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
>
> Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
>
> Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the

[47] *Id.* at 3-4.

> AppData/LocalAppData folder.
>
> Consider disabling Remote Desktop protocol (RDP) if it is not being used.
>
> Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
>
> Execute operating system environments or specific programs in a virtualized environment.
>
> Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

119. Further, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, or ensured PSC implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:[48]

> **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
>
> **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (*e.g.*, contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (*e.g.*, .com instead of .net)….
>
> **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
>
> **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender

[48] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against- ransomware

> directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….

120. In addition, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, or ensured that PSC implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:[49]

a. Secure internet-facing assets

   1) Apply latest security updates

   2) Use threat and vulnerability management

   3) Perform regular audit; remove privileged credentials

b. Thoroughly investigate and remediate alerts

   1) Prioritize and treat commodity malware infections as potential full compromise;

c. Include IT Pros in security discussions

   1) Ensure collaboration among [security operations], [security

[49] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated- ransomware-attacks-a-preventable-disaster/.

admins], and [information technology] admins to configure servers and other endpoints securely;

d. Build credential hygiene

1) Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

e. Apply principle of least-privilege

1) Monitor for adversarial activities

2) Hunt for brute force attempts

3) Monitor for cleanup of Event Logs

4) Analyze logon events

f. Harden infrastructure

1) Use Windows Defender Firewall

2) Enable tamper protection

3) Enable cloud-delivered protection

4) Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].

121. Given that Defendant utilized the MOVEit transfer tool, which stored the Private Information of thousands of individuals, including Plaintiff and the Class Members, Defendant could and should have ensured that the MOVEit software was capable of preventing and detecting cyber-security attacks.

122. To prevent zero-day attacks, Defendant could and should have implemented, or ensured PSC implemented, as recommended by Security Intelligence, the following:[50]

[50] *See* Jonathan Reed, *The MOVEit breach impact and fallout: How can you respond?*, July 19,

> **Patch management:** Formal patch management can help security teams remain aware of critical patches.
>
> **Vulnerability management:** Vulnerability assessments and penetration tests can help companies detect zero-day vulnerabilities before adversaries find them.
>
> **Attack surface management (ASM):** ASM enables security teams to identify all network assets and scan them for vulnerabilities. ASM tools assess the network from an attacker's perspective, focusing on how threat actors might try to exploit assets.
>
> **Threat intelligence:** Security researchers are often the first to identify zeroday vulnerabilities. Organizations that receive threat intelligence updates may be informed about zero-day vulnerabilities sooner.
>
> **Anomaly-based detection methods**: Machine learning tools can spot suspicious activity in real-time. Common anomaly-based detection solutions include user and entity behavior analytics (UEBA), extended detection and response (XDR) platforms, endpoint detection and response (EDR) tools and some intrusion detection and intrusion prevention systems.

123. Defendant acquired, collected, and stored the Private Information of Plaintiff and Class Members.

124. Plaintiff and other Members of the Class entrusted their Private Information to Defendant.

125. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII/PHI from disclosure.

126. Given that Defendant was storing the Private Information of other individuals, Defendant could and should have implemented all of the above measures, and ensured that PSC did the same, to prevent and detect cyber-security attacks.

127. The occurrence of the Data Breach indicates that Defendant failed to adequately

---

2023, The MOVEit breach impact and fallout: How can you respond? (securityintelligence.com).

implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

128. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and data fields containing the Private Information of Plaintiff and Class Members and ensuring the MOVEit software properly secured and encrypted the folders, files, and/or data fields containing the Private Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data that it no longer had a reasonable need to maintain, or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

129. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

130. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

F. Defendant's Response to and Notice of the Data Breach is Inadequate to Protect Plaintiff and the Class

131. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

132. Defendant stated that "[o]n May 31, 2023, the software of one of our vendors was hacked by a bad actor. We use MOVEit software to share data to manage your benefits. We

patched the software as instructed on June 1."[51] Further, by June 27, 2023, CareSource confirmed that its customers' data had been hacked.[52] Despite the public notices published by PSC, and Defendant's awareness of its use of PSC's MOVEit tool, CareSource did not notify Plaintiff until on or about September 14, 2023 —over two months after CareSource had definitive knowledge of the breach.

133. During these intervals, the cybercriminals had the opportunity to exploit Plaintiff's and Class Members' Private Information while Defendant was sitting idle.

G. Defendant Failed to Comply with FTC Guidelines

134. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

135. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[53] The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the

[51] https://www.caresource.com/about-us/legal/corporate-compliance/vendor-compliance/ hipaa-hitech/cybersecurity-incident/
[52] *Id.*
[53] https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protecting persinfo-508.pdf

system; and have a response plan ready in the event of a breach.

136. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

137. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C.

138. Defendant was always fully aware of their obligations to protect the Private Information of Plaintiff and Class Members and the significant repercussions that would result from its failure to ensure the MOVEit software had adequate data security.

H. CareSource Failed to Adhere to HIPAA

139. HIPAA contains security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[54]

140. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and

[54] HIPAA lists 18 types of information that qualifies as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

security of PHI is properly maintained.[55]

141. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the MOVEit software was capable of maintaining the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to ensure the MOVEit software was capable of protecting against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §164.306(a)(2);

c. Failing to ensure that the MOVEit software was capable of protecting against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

d. Failing to comply with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. §164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

[55] *See* 45 C.F.R. § 164.306 (Security standards and General Rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308; and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. §164.530(c).

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of the Nationwide Class and the Ohio Subclass)

142. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

143. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PHI of Plaintiff and Class Members in its computer systems and on its networks.

144. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI in its possession;

b. to protect Plaintiff's and Class Members' PHI using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI.

145. Defendant knew that the PHI was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

146. Defendant knew, or should have known, of the risks inherent in collecting and storing PHI, the vulnerabilities of its data security systems, and the importance of adequate security.

147. Defendant knew about numerous, well-publicized data breaches.

148. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PHI.

149. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI that Plaintiff and Class Members had entrusted to it.

150. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard

their PHI.

151. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PHI contained therein.

152. Plaintiff's and Class Members' willingness to entrust Defendant with their PHI was predicated on the understanding that Defendant would take adequate security precautions.

153. Moreover, only Defendant had the ability to protect its systems and the PHI is stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

154. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PHI and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiff, and/or the remaining Class Members.

155. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI of Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PHI had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured

PHI;

d. by failing to provide adequate supervision and oversight of the PHI with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI of Plaintiff and Class Members, misuse the PHI and intentionally disclose it to others without consent.

e. by failing to adequately train its employees not to store PHI longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PHI;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiff's and Class Members' PHI and monitor user behavior and activity in order to identify possible threats.

156. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

157. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

158. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI.

159. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

160. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

161. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI.

162. There is a close causal connection between Defendant's failure to implement security measures to protect the PHI of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

163. Plaintiff's and Class Members' PHI was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

164. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

165. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

166. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI is used; (iii) the

compromise, publication, and/or theft of their PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) lost continuity in relation to their healthcare; (vii) the continued risk to their PHI, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PHI in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

167. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

168. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI in its continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of the Nationwide Class and the Ohio Subclass)

169. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

170. Through its course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI.

171. Defendant required Plaintiff and Class Members to provide and entrust their PHI as a condition of obtaining Defendant's services.

172. Defendant solicited and invited Plaintiff and Class Members to provide their PHI as part of Defendant's regular business practices.

173. Plaintiff and Class Members accepted Defendant's offers and provided their PHI to Defendant.

174. As a condition of being direct patients of Defendant, Plaintiff and Class Members provided and entrusted their PHI to Defendant.

175. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

176. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PHI to Defendant, in exchange for, amongst other things, the protection of their PHI.

177. Plaintiff and Class Members fully performed their obligations under the implied

contracts with Defendant.

178. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PHI and by failing to provide timely and accurate notice to them that their PHI was compromised as a result of the Data Breach.

179. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class and the Ohio Subclass)

180. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

181. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

182. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

183. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and

continued acceptance of PHI and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

184. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of the Nationwide Class and the Ohio Subclass)

185. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

186. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

187. Defendant, prior to and at the time Plaintiff and Class Members entrusted their PHI to Defendant for the purpose of obtaining health services, caused Plaintiff and Class Members to reasonably believe that Defendant would keep such PHI secure.

188. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their PHI kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

189. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

190. Defendant failed to disclose facts pertaining to its substandard information

systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

191. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiff and Class Members the ability to make a rational and informed health care decision and took undue advantage of Plaintiff and Class Members.

192. Defendant was unjustly enriched at the expense of Plaintiff and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for health care services that did not satisfy the purposes for which they bought/sought them.

193. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

194. Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

COUNT FIVE
Invasion of Privacy
(On Behalf of Plaintiff and the Ohio Sublass)

195. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged herein.

196. Plaintiff and Class Members have a reasonable expectation of privacy in their Private Information.

197. Defendant's negligent, reckless, and intentional conduct as alleged herein invaded Plaintiff's and Class Members' privacy.

198. By knowingly failing to keep Plaintiff's and Class Members' Private Information safe, and by knowingly misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant negligently, recklessly, and intentionally invaded Plaintiff's and Class Members' privacy by intruding into Plaintiff's and Class Members' private affairs, without approval, in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to a person of ordinary sensibilities.

199. Defendant knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendant's negligent, reckless, and intentional actions highly offensive and objectionable.

200. Such an intrusion into Plaintiff's and Class Members' private affairs is likely to cause outrage, shame, and mental suffering because the Private Information disclosed contained PII and PHI.

201. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private life by negligently, recklessly, and intentionally

misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

202. The Private Information disclosed by Defendant has no legitimate reason to be known by the public.

203. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

204. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests, caused anguish and suffering such that a person with ordinary sensibilities would consider Defendant's intentional actions or inaction highly offensive and objectionable.

205. In failing to protect Plaintiff's and Class Members' Private Information, and in negligently, recklessly, and intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

COUNT SIX
Breach of Confidentiality
(On Behalf of Plaintiff and the Ohio Subclass)

206. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged herein.

207. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information.

208. Plaintiff's and Class Members' Private Information constitutes confidential and novel information. For example, Plaintiff's and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Similarly, Plaintiff and Class Members cannot change their medical histories.

209. As alleged herein and above, Defendant's relationships with Plaintiff and Class Members were governed by terms and expectations that Plaintiff's and Class members' Private Information would be collected, stored, and protected in confidentiality, and would not be disclosed to unauthorized third parties.

210. Plaintiff and Class Members provided their respective Protected Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

211. Defendant voluntarily received in confidentiality Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

212. Due to Defendant's failure to ensure the MOVEit software was capable of preventing, detecting, and avoiding the Data Breach from occurring by, *inter alia*, not following best information security practices and by not providing proper training to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

213. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

214. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information through its use of unsecured systems in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

215. This disclosure of Plaintiff's and Class Members' Private Information constituted a violation of Plaintiff's and Class Members' understanding that Defendant would safeguard and protect the confidential and novel Private Information that Plaintiff and Class Members were required to disclose to Defendant.

216. The concrete injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew or should have known that the MOVEit

software's data security measures had numerous security and other vulnerabilities that placed Plaintiff's and Class Members' Private Information in jeopardy.

217. As a direct and proximate result of Defendant's breaches of confidentiality, Plaintiff and Class Members have suffered and/or are at a substantial risk of suffering concrete injury that includes but is not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII/PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII/PHI; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect the Private Information under its continued control; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and each member of the proposed National Class and the Ohio Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as

Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge the PHI of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and

integrity of Plaintiff's and Class Members' PHI;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

f. prohibiting Defendant from maintaining Plaintiff's and Class Members' PHI on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI, as well as protecting the PHI of Plaintiff and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks

for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Date: September 25, 2023

Respectfully submitted,

REESE LLP

/s/ Michael R. Reese
Michael R. Reese
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500
Email: *mreese@reesellp.com*

REESE LLP
Charles D. Moore
121 N. Washington Ave, 4th Floor
Minneapolis, Minnesota 55401
Telephone: 212-643-0500
Email: *cmoore@reesellp.com*

Attorneys for Plaintiff and the Proposed Class